Contract on order processing according to Art. 28 GDPR

between

Company
Street
Location

represented by
company management
Mr./Mrs./Miss

in the following: **customer**

and

Infopark Group GmbH
Kitzingstraße 15
12277 Berlin

represented by
company management
Bernd Völcker

in the following: **contractor**

§ 1 Introduction, scope, definitions

(1) This contract regulates the rights and obligations of both the customer and contractor, in the context of the processing of personal data in the order.

(2) This contract shall apply to all activities in which employees of the contractor or subcontractors assigned by the contractor process a customer's personal data.

(3) Terms used in this contract are to be understood according to their definition in the EU General Data Protection Regulation (GDPR). Insofar as declarations in the following are to be made "in writing", the written form according to § 126 German Civil Code (BGB) is meant. In addition, declarations may also be made in another form, provided that appropriate verifiability is ensured.

§ 2 Subject and duration of processing

(1) The processing is based on the order/contract (hereinafter referred to as "main contract") consisting between the parties. The subject of the order processing results from the main contract.

(2) The duration of this contractual agreement is based on the duration of the main contract. A termination of the main contract automatically results in a termination of this contractual agreement.

§ 3 Type of processed data, circle of affected

(1) In the course of the execution of the main contract, the contractor shall be granted access to the personal data specified in **annex 1**.

(2) The circle of subjects affected by the data processing is also presented in **annex 1**.

§ 4 Scope and responsibilities

(1) The contractor processes personal data on behalf of the customer. This includes activities that are specified in the contract and in the service description. Within the scope of this contract, the customer shall be solely responsible for compliance with the statutory provisions of the data protection laws, in particular for the lawfulness of the data transfer to the contractor and for the lawfulness of the data processing ("Responsible Party" in the sense of Art. 4 No. 7 GDPR).

(2) The provision of the contractually agreed data processing, takes place exclusively in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the customer and may only take place if the special conditions of Art. 44 ff. GDPR are fulfilled.

(3) The instructions are initially set out in the contract and may subsequently be amended, supplemented or replaced by individual instructions by the customer in writing or in an electronic format (text form) to the body designated by the contractor (individual instructions). Instructions which are not provided for in the contract are treated as a request for a change in service. Oral instructions must be confirmed immediately in writing or in text form.

(4) Insofar as instructions or notices are to be given under this contractual agreement, they shall be addressed to the persons listed in **annex 4**. Each party may change the contact persons by a declaration in text form to the other party. The change shall become effective immediately upon receipt of the declaration of change.

(5) If individual instructions entail additional costs, in particular if these exceed the contractually agreed scope of services, these are to be reimbursed to the contractor.

§ 5 Obligations of the contractor

(1) The contractor may only process data of data subjects within the scope of the order and the instructions of the customer, unless there is an exceptional case in the sense of Article 28 para. 3 a) GDPR. The contractor shall inform the customer without delay, if he believes that an instruction violates applicable laws. The contractor may suspend the implementation of the instruction until it has been confirmed or amended by the customer.

(2) Within his area of responsibility, the contractor will design the internal organization in such a way that it meets the special requirements of data protection. He will take technical and organizational actions for the appropriate protection of the customer's data which meet the requirements of the General Data Protection Regulation (Art. 32 GDPR). The contractor shall take technical and organizational actions to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing in the long term.

(3) The contractor commits to the customer to comply with the technical and organizational actions specified in **annex 2**, which are necessary to comply with the applicable data protection regulations. The contractor reserves the right to change the security measures taken. In doing so, however, the security level may not fall below the security level of the specified measures.

(4) The contractor shall assist the customer in complying with the obligations regarding the security of personal data set out in Articles 32 to 36 of the GDPR, reporting obligations in the event of

data breaches, data protection impact assessments and prior consultations. The contractor may claim remuneration for support services that are not included in the service description or are not due to misconduct on the part of the contractor.

(5) The contractor guarantees that the employees involved in the processing of the customer's data and other persons working for the contractor are prohibited from processing the data outside of the instruction. Furthermore, the contractor shall ensure that the persons authorized to process the personal data have undertaken to maintain confidentiality or are subject to an appropriate statutory duty of confidentiality. The confidentiality obligation shall continue to exist after the termination of the order.

(6) The contractor shall inform the customer without delay if he becomes aware of violations of the customer's personal data protection. The contractor shall take the necessary actions to secure the data and to mitigate any adverse consequences of the persons concerned and shall consult with the customer without delay.

(7) The contractor has appointed a qualified data protection officer, whose name and contact details, must be noted in **annex 4.**

(8) The contractor guarantees to comply with his obligations under Art. 32 para. 1 lit. d) GDPR to implement a procedure to regularly check the effectiveness of the technical and organizational measures to ensure the security of the processing.

(9) In the event of a claim against the customer by an affected person with regard to any claims under Art. 82 GDPR, the contractor shall bear the burden of proof under Art. 82 GDPR, the obligations to cooperate under Art. 28 GDPR as well as the generally applicable accountability and transparency obligations under Art. 5. The contractor commits to support the customer in defending the claim within the scope of its statutory obligations and with regard to its joint liability.

§ 6 Obligations of the customer

(1) The customer must inform the contractor immediately and completely, if he discovers errors or irregularities in the order results with regard to data protection regulations.

(2) In the event of a claim against the customer by a person concerned with regard to any claims under Art. 82 GDPR, §5 para. 9 shall apply accordingly.

(3) The customer shall name the contact person for data protection issues arising within the scope of the contract to the contractor in **annex 4**.

§ 7 Requests from data subjects

(1) If a data subject turns to the contractor with requests for rectification, deletion or information, the contractor shall refer the data subject to the customer, provided that an attribution to the customer is possible according to the data subject. The contractor shall forward the data subject's request to the customer without delay. The contractor shall support the customer within the scope of his possibilities on instruction to the extent agreed. The contractor shall not be liable if the request of the person concerned is not correctly, or not timely answered by the customer.

(2) The customer shall reimburse the contractor for any incurred and proven expenses and costs in providing the support services pursuant to paragraph 1.

§ 8 Control rights of the customer

(1) The customer shall convince himself of the contractor's technical and organizational measures before starting data processing and then regularly thereafter. For this purpose, he may, for example, obtain information from the contractor, have existing attestations from experts, certifications or internal audits presented to him or personally check the technical and organizational procedures of the contractor during normal business hours or have them checked by a competent third party. Provided that the latter is not in a competitive relationship with the contractor. The customer shall only carry out inspections to the extent necessary and shall not disrupt the contractor's operating procedures disproportionately. The customer shall give at least two weeks advance notice of any unannounced on-site inspections; unannounced on-site inspections may be carried out once per calendar year.

(2) Upon request, the contractor shall provide the customer with all information necessary to prove compliance with the obligations under this agreement and to fulfill existing data protection obligations, including accountability. For this purpose, the contractor shall guarantee the customer the rights of access, information and inspection required by the contractor for the performance of the inspection. In particular, the contractor shall commit himself to grant the customer access to the data processing facilities and other documents in order to enable the control and inspection of the relevant data processing facilities and other documentation related to the collection or processing of data of the customer. In doing so, the customer shall show consideration for the operating procedures and legitimate secrecy interests of the contractor.

§ 9 Subcontractors

(1) The use of subcontractors as further processors is only permitted if the customer has given his prior consent. The same applies to the replacement of an existing subcontractor.

(2) A subcontracting relationship requiring approval shall be deemed to exist, if the contractor commissions further contractors with the complete or partial performance of the service agreed in the contract. The contractor shall enter into agreements with these third parties to the required extent, in order to ensure appropriate data protection and information security procedures. No consent is required for the involvement of subcontractors where the subcontractor solely uses an ancillary service to support the performance of the services under the main contract, even if access to the customer's data cannot be excluded; this includes in particular telecommunications services, postal or transport services, maintenance and user service or the disposal of data carriers as well as other steps to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The contractor shall enter into non-disclosure agreements with such subcontractors that are customary in the industry.

(3) Such prior consent may only be refused by the customer for good cause, which must be proven to the contractor.

(4) The customer agrees to the commissioning of the subcontractors listed in **annex 3**, subject to a contractual agreement in accordance with Art. 28 para. 2-4 GDPR.

§ 10 Termination of the main contract

(1) The customer may terminate the main contract as well as this contract without observing any notice periods if there is a serious, culpable violation by the contractor of data protection regulations or provisions of this contract, if the contractor disregards legitimate instructions of the customer, or if the contractor refuses access by the customer or a correspondingly authorized person to the business premises where data are processed on the basis of this contract in violation of the contract.

(2) The contractor shall return to the customer all documents, data and data carriers made available to him, after termination of the main contract or at any time at the customer's request or, at the customer's request, completely destroy or irrevocably delete all personal data unless the contractor is obliged to store such data under Union law or the law of a Member State. This also concerns any data backups at the contractor.

(3) The deletion/destruction is to be documented in a suitable manner - for example by means of a protocol. The documentation of the deletion/destruction shall be presented on request.

(4) The contractor is obliged to treat confidentially all data that has become known to him in connection with the main contract even after the end of the main contract. The present contractual agreement shall remain valid beyond the end of the main contract, as long as the contractor has personal data at his disposal which have been provided to him by the customer or which he has collected for the contract.

§ 11 Duty to inform, written form clause, choice of law

(1) If the data of the customer are endangered by the contractor either by seizure or confiscation, by insolvency or composition proceedings or by other events or actions of third parties, the contractor must inform the customer immediately. The contractor shall inform all persons responsible in this context without delay that the sovereignty and ownership of the data lie exclusively with the customer as "responsible person" in the sense of the General Data Protection Regulation.

(2) Amendments and supplements to this contractual agreement and all of its components, including any assurances given by the contractor, require a written agreement, which may also be in an electronic format (text form), and the explicit indication that this is an amendment or supplement to these terms and conditions. This also applies to the waiver of this formal requirement.

(3) In the event of any contradictions, provisions of this contractual agreement on data protection shall take precedence over the provisions of the contract. Should individual parts of this contractual agreement be invalid, this shall not affect the validity of the contractual agreement.

(4) German law applies.

Location, _____

(customer)

Berlin, _____

(contractor)

Annex 1 Description of the personal data / data categories and description of the categories of data subjects

Annex 2 Technical and organizational actions of the contractor

Annex 3 Approved subcontractors

Annex 4 Authorized persons and recipients of instructions and contact details of the data protection officers

Annex 1

Description of the personal data / data categories and description of the categories of data subjects

1. Data types/categories processed

The following types or categories of data are subject to the processing of orders:

- Personal master data (e.g. first name and surname)
- Communication data (e.g. telephone, email)
- Address data
- IP address
- Applicant data (e.g. diplomas, certificates, references)
- Contract master data (contractual relationship, product or contract interest)
- Contract billing and payment data
- Customer history
- Bank details
- Credit card details
- IT data (e.g. IT user names, log files, access rights)
- Support ticket data (e.g. help desk or customer support ticket system)

2. Description of the categories of data subjects

The following categories of persons (holder/owner of the data) are concerned by the processing of orders:

- Customers
- Contact person
- Interested parties
- Subscribers
- Suppliers
- Applicants

3. Scope, kind and purpose of the processing of personal data

The following services are provided within the scope of order processing. The contractor carries out the following processing:

- Storage of content for the websites of the customer in Scrivito
- Storage of customer data (exact data will be determined in the concrete project and are subject to change)
- Storage of contacts for authentication and authorization in Scrivito (and on website)
- Processing explicitly commissioned by the customer, e.g. error analysis in case of need

The processing serves the following purpose:

- Content editing and delivery (e.g. through the Content Management System Scrivito)
- Authentication, authorization, user data management (e.g. change master data and password)
- Error analysis
- Availability monitoring
- Performance analysis
- Analysis of customer visits and optimization of the website
- Interested parties/lead acquisition on websites (e.g. contact forms, newsletter signup etc.)

Annex 2

General description of the technical and organizational procedures

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

The risk of physical, material or non-material damage or the risk of impairment of the rights and freedoms of data subjects must be reduced.

Access control (Office)

Technical and organizational actions

- Access control to the server rooms is guaranteed by the spatial structure of the respective data center and the control systems used by the operator.
- During business hours, access to the premises of Infopark Group GmbH in Berlin, is ensured by an individualized electronic key (transponder).
- Outside business hours, the rooms are permanently monitored by an external service provider (security service, closing of doors and motion detection).
- In addition, the external doors of the building are mechanically closed outside of business hours.
- During business hours, access is controlled by personnel in the reception area.
- Entrance areas and the technical area are permanently controlled by optical room surveillance (video).

Access control (IT-Accounts)

Technical and organizational actions:

- The unauthorized use of the data processing systems is prevented by:
  - password assignment and
  - Two-factor authentication (where possible)
  - Security requirements for passwords (where possible).
- Each authorized person has his own secure/long passwords per service, known only to him, which must not be passed on and are managed by a central password manager. If the password becomes known, it must be changed immediately.
- Whenever possible, a two-factor authentication is mandatory.
- Protocols are automatically created for all relevant activities on the DP system.
- The protocols are regularly analyzed by the system administrator on a random sample basis as well as in case of abnormalities (e.g. particularly high activity).
- During critical activities (e.g. system maintenance, software updates, backups), data transfer to and from the DP system is protected against unauthorized use by the following actions:

- Verification of known public keys when contact is made (if possible);
- Encrypted data transmission (SSH/TLS - where possible via public/private key authentication);
- Logging of system usage and protocol evaluation.

Access control (Data)

Technical and organizational actions:

- Unauthorized reading, copying, modification or deletion of data media is prevented by:
  - software exclusion (authorization concept);
  - software-based monitoring of implausible usage (monitoring);
  - secured interfaces;
  - further control mechanisms of the data centre.
- Authorizations are only granted by a small circle of management employees according to the least privilege principle.
- Mobile data storage devices must not be used. Mobile backup media are not used for service.
- No data storage devices are kept at the workplace or in the business premises. Developers only have access to fictitious test data. Personnel charged with fault clearance can access real access data as far as this is necessary for fault clearance.
- The restriction of the access possibility of the person authorized to use a data processing system exclusively to the data subject to his access is guaranteed by:
  - automatic verification of access authorization by means of a password;
  - exclusive menu control depending on authorization;
  - differentiated access authorization to application programs;
  - differentiated processing options (read/change/delete).

Separation Control

Technical and organizational actions:

- Personal data may only be used for the purpose for which it was originally collected.
- The fact that data collected for different purposes can be processed separately is guaranteed by:
  - software exclusion (client separation; multi-tenancy architecture);
  - separation via access control;
  - separation of test and production data;
  - separation of development and production environments.

Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

Technical and organizational actions:

- Infopark Group GmbH, as the processor of the order, does not take any further steps for pseudonymization in addition to the actions taken by the responsible person within the scope of the order.

2. Integrity (Art. 32 para. 1 lit. b GDPR)

Transfer control

Technical and organizational actions:

- The policy does not include physical dispatch of data storage media.
- Private data storage media must not be used in the datacenter (datacenter policy).
- Magnetic data storage media that are no longer needed are destroyed by multiple overwrites (datacenter policy).
- Unauthorized reading, copying, modification or removal of data during data transmission is prevented by:
  - SSL, i.e. SSH encryption during data transmission;
  - Completeness checks, where relevant;
  - Establishment of transport connections only between defined systems secured by certificates.
- The transport procedures automatically confirm receipt of data in the software.
- All sensitive data intended for transport is encrypted.
- Personal data is only transmitted using the following services:
  - Routinely WWW (HTTPS);
  - Other services and transport procedures that satisfy the intended purposes and are equivalent to or better than the current state-of-the-art in security technology.
- The documentation of transmission points and pathways provides information on the points at which data transmission systems are used to transmit data.

Input control

Technical and organizational actions:

- Whether and by whom data have been entered, changed or removed from data processing systems can be subsequently checked and determined by
  - user identification;
  - logging of entered data (processing protocol).

3. Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

The risk of physical, material or immaterial damage or the risk of impairment of rights and freedoms, including through unlawful or negligent acts, for data subjects due to unavailability of data processed under the contract must be reduced.

Availability control

Technical and organizational actions:

- The protection of data against accidental destruction or loss is ensured by:
  - Distributed data storage and processing across several physically separate computer centers locations;
  - Regular database and system backups;
  - Additional steps taken by the computer center.
- A plan for the event of a disaster is provided.

Load capacity of the systems

Technical and organizational actions:

- The following security procedures exist:
  - Firewalls and virtual private networks;
  - Intrusion Detection System;
  - Programs that prevent the intrusion of viruses or detect the intrusion.

4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Procedures shall be in place to regularly review, assess and evaluate the effectiveness of the technical and organizational measures to ensure the security of processing.

Order Control

Technical and organizational actions:

- No processing of orders in the sense of Art. 28 GDPR will be carried out without corresponding instructions from the customer, e.g. clear contract design, formalized order management, strict selection of the service provider, obligation of prior conviction as well as follow-up checks.
- The processing of personal data in the order only according to the instructions of the customer is guaranteed by written agreements on data protection between customer and contractor or computer center.
- The customer will be informed by the contractor about serious changes in the course of the procedure.

- The backup of the distance maintenance is not necessary, because no distance maintenance at the client is planned.

Internal organisation

Technical and organizational actions:

(a) Data protection management

- Only employees who have been obliged to comply with data protection regulations may process the data corresponding to their area of responsibility.
- There are internal guidelines for conduct and a data protection manual.
- All employees are trained and sensitized at regular intervals on the subject of data protection.
- An organization chart and job descriptions define responsibilities and authorities of individual employees and made known within the company. This is checked at regular intervals by top management as part of the ISO 9001 certification.

(b) Incident management

- Compliance with the technical and organizational procedures is checked annually by the data protection officer and adjusted if necessary (audit).

(c) Data protection through technology design

- Selection of privacy friendly technology for procurement

Annex 3

Approved subcontractors

The following companies are approved subcontractors.

Address of the subcontractor	Service	Countries where data are processed
Amazon Web Services, Inc. 410 Terry Avenue North Seattle, WA 98109, USA	Hosting and operation	USA
Github Inc. 88 Colin P Kelly Jr St San Francisco, CA 94107, USA	Source code management	USA
Google, Inc. 1600 Amphitheatre Pkwy Mountain View CA 94043, USA	Email communication	USA
Honeybadger Industries LLC 11410 NE 124th Street #246, Kirkland, WA 98034, USA	Error Tracking	USA
Intercom R&D Unlimited Company 18-21 St. Stephen's Green Dublin 2, Irland	Chat Communication	Ireland
Loggly, Inc. 535 Mission St, Ste 2100 San Francisco, CA 94105, USA	Log analysis and monitoring	USA
Netlify Inc. 2325 3rd Street, Suite 215 San Francisco, CA 94107, USA	Hosting JavaScript and HTML code	USA
Netsuite / Oracle Inc. 500 Oracle Parkway Redwood Shores, CA, 94403, USA	Accounting/ ERP	USA

Pingdom AB Kopparbergsvägen 8 72213 Västerås, Schweden	Availability/Performance Monitoring	Sweden
Segment.io, Inc. 100 California Street, Suite 700 San Francisco, CA 94111, USA	Service orchestration Analytics	USA
Slack Technologies, Inc. 155 5th St, 6th Floor San Francisco, CA 94103, USA	Chat Communication	USA
Stripe, Inc. 510 Townsend Street San Francisco, CA 94103, USA	Payment transactions	USA

Annex 4

Authorized persons and recipients of instructions and contact details of the data protection officers

In the event of a change or a long-term blockage of the contact persons, the contractual partner must be informed of the successors or representatives.
(Please enter data):

1. Authorized representatives and recipients of instructions

Customer

Name	Telephone	Email

Contractor

Name	Telephone	Email

2. Data protection officer

Customer

Name	Telephone	Email

Contractor

Stephan Hartinger Coseco GmbH	+49 8232 80988-70	datenschutz@coseco.de